KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_2a73cad53d7b.exe

Verdict: MALICIOUS

Verdict: likely-malicious; 78 anti-VM checks (mixed)

Analysis Overview

Score: 8/10

Threat level: Malicious

Malicious Activity Summary

- T1497.001
- T1105
- Obfuscated Files or Information
- Process Injection
- Process Injection: Dynamic-link Library Injection
- Input Capture: Keylogging
- Process Discovery
- Indicator Removal: File Deletion
- Application Layer Protocol: Web Protocols
- Native API
- Modify Registry
- Screen Capture
- Clipboard Data
- Shared Modules
- Access Token Manipulation
- Data Encrypted for Impact
- Credentials from Password Stores: Credentials from Web Browsers
- Hijack Execution Flow: DLL Side-Loading
- Debugger Evasion
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	2a73cad53d7b6ee5df6fce0d9f5761891c6bf42d674130dab5a634ffcd9b3423
SHA-1:	0045f51bbd0f4285fc59b60f9652e6a6ad0f8242
MD5:	f3053fed83a4d313e8aa9cace5db69ab
Size:	641,536 bytes

Packer Detection

No packer detected.

PE Information

Architecture: 64-bit

Type: Executable

Entry Point: 0x49A34

Sections: 6

Name	Virtual Size	Entropy
.text	0x6EF58	6.43
.rdata	0x20662	5.43
.data	0xC7F4	2.91
.pdata	0x62DC	5.66
.rsrc	0x4AE0	3.98
.reloc	0xDA0	5.39

Imports

KERNEL32.dll

- GetLogicalDriveStringsA
- SetFilePointerEx
- MoveFileW
- RemoveDirectoryW
- GetModuleHandleA
- TerminateThread
- GetFileSize
- ExpandEnvironmentStringsW
- GetEnvironmentVariableW
- MultiByteToWideChar

USER32.dll

- wsprintfW
- GetClipboardData
- UnhookWindowsHookEx
- GetForegroundWindow
- ToUnicodeEx
- GetKeyboardLayout
- SetWindowsHookExA
- CloseClipboard
- OpenClipboard
- GetKeyboardState

GDI32.dll

- BitBlt
- CreateCompatibleBitmap
- SelectObject
- CreateCompatibleDC
- StretchBlt
- GetDIBits
- DeleteDC
- DeleteObject
- CreateDCA
- GetObjectA

ADVAPI32.dll

- CryptAcquireContextA
- CryptGenRandom

CryptReleaseContext
GetUserNameW
RegEnumKeyExA
GetTokenInformation
AdjustTokenPrivileges
LookupPrivilegeValueA
OpenProcessToken
RegQueryInfoKeyW

SHELL32.dll

Shell_NotifyIconA
ShellExecuteExA
ShellExecuteW
ExtractIconA

ole32.dll

CoUninitialize
CoGetObject
CoInitializeEx

WINMM.dll

waveInOpen
waveInUnprepareHeader
waveInPrepareHeader
waveInStop
waveInStart
waveInAddBuffer
mciSendStringW
mciSendStringA
PlaySoundW
waveInClose

WS2_32.dll

socket
connect
recv
send
WSAGetLastError
WSAStartup
getaddrinfo
inet_ntoa
closesocket

urlmon.dll

URLOpenBlockingStreamW
URLDownloadToFileW

gdiplus.dll

GdipLoadImageFromStream
GdipDisposeImage
GdipAlloc
GdipSaveImageToStream
GdipGetImageEncodersSize
GdipCloneImage
GdipGetImageEncoders
GdiplusStartup
GdipFree

WININET.dll

InternetReadFile

InternetCloseHandle
InternetOpenW
InternetOpenUrlW

Strings (200 found)

```
!This program cannot be run in DOS mode.
K:s`B;
K:s`
K:s`I;
K:Rich
.text
`.rdata
@.data
.pdata
@.rsrc
@.reloc
x AVH
\$@H
l$HH
t$PH
|$XH
\$0H
t$8H
D$@H
L$`L
T$ H
T$HH
UVWAVAWH
t$ D
t$ D
t$ D
t$ D
t$ D
t$ E
t$ E
t$ D
t$ D
t$ E
t$ E
t$ D
t$ D
t$ D
PA_A^_^]
\$0H
\$0H
t$8H
\$0H
\$0H
\$0H
\$0H
\$0H
\$0H
\$0H
t$8H
```

`\$8H`

`\$0H`

... and 150 more

Malware Config

C2 / Network (1)

Endpoint	Source
`108.181.253.47:443`	network

Indicators of Compromise (7)

IPv4 addresses (1)

`108.181.253.47`

Domains (6)

`zaa.co`

`ccu.cc`

`api.msn.com`

`assets.msn.com`

`www.bing.com`

`arc.msn.com`

MITRE ATT&CK (20)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1105			detonation-evidence
T1027	Obfuscated Files or Information	Defense Evasion	
T1055	Process Injection	Defense Evasion	
T1055.001	Process Injection: Dynamic-link	Defense Evasion	
T1056.001	Input Capture: Keylogging	Credential Access	
T1057	Process Discovery	Discovery	
T1070.004	Indicator Removal: File Deletion	Defense Evasion	
T1071.001	Application Layer Protocol: Web	Command and Control	
T1106	Native API	Execution	
T1112	Modify Registry	Defense Evasion	
T1113	Screen Capture	Collection	
T1115	Clipboard Data	Collection	
T1129	Shared Modules	Execution	
T1134	Access Token Manipulation	Privilege Escalation	
T1486	Data Encrypted for Impact	Impact	
T1555.003	Credentials from Password Stores	Credential Access	
T1574.002	Hijack Execution Flow: DLL Side-	Privilege Escalation	
T1622	Debugger Evasion	Defense Evasion	
T1547.001	Boot or Logon Autostart Executio	Persistence	behavioral_inference

Dynamic Detonation

Coverage: ran

Behavior: malicious-behavior

Threat score: 80/100 (high)

Factors: c2, beaconing, attack_techniques

C2 beaconing: 1

Network Connections (9)

Destination	Domain	Proto
10.0.2.3:443		tcp
10.0.2.3:80		tcp
108.181.253.47:443		tcp
10.0.2.3:53		udp
10.0.2.255:137		udp
224.0.0.251:5353		udp
10.0.2.255:138		udp
255.255.255.255:67		udp
224.0.0.252:5355		udp

TLS Handshake Failures (cert-pinning) (50)

```
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
www.bing.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
```

Behavioral Timeline (100)

1. [conn] pid 0: udp 255.255.255.255:67
2. [conn] pid 0: udp 224.0.0.251:5353
3. [conn] pid 0: udp 224.0.0.252:5355
4. [conn] pid 0: udp 10.0.2.255:137
5. [conn] pid 0: udp 224.0.0.252:5355
6. [conn] pid 0: udp 10.0.2.3:53
7. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
8. [conn] pid 0: tcp 10.0.2.3:80
9. [conn] pid 0: udp 10.0.2.3:53
10. [dns] pid 0: DNS 1 login.live.com -> 10.0.2.3
11. [conn] pid 0: tcp 10.0.2.3:443
12. [conn] pid 0: udp 10.0.2.3:53
13. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3

14. [conn] pid 0: tcp 10.0.2.3:80
15. [conn] pid 0: tcp 10.0.2.3:80
16. [conn] pid 0: tcp 10.0.2.3:80
17. [conn] pid 0: tcp 10.0.2.3:443
18. [conn] pid 0: tcp 10.0.2.3:80
19. [conn] pid 0: tcp 10.0.2.3:80
20. [conn] pid 0: tcp 10.0.2.3:443
21. [conn] pid 0: tcp 10.0.2.3:80
22. [conn] pid 0: tcp 10.0.2.3:80
23. [conn] pid 0: tcp 10.0.2.3:80
24. [conn] pid 0: tcp 10.0.2.3:443
25. [conn] pid 0: tcp 10.0.2.3:80

...and 75 more events

Packet capture: available (full PCAP)

Persistence (1)

```
[Startup folder] malray.bat -> /ProgramData/Microsoft/Windows/Start Menu/Programs/Startup/malray.bat
```

Spawned Processes (50)

```
System
Registry
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p
smss.exe - \SystemRoot\System32\smss.exe
StartMenuExper - "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceH
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{133EAC4F-5891-4D04-BADA-D84870380A80}
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
SearchApp.exe - "C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe" -ServerName:CortanaUI.A
svchost.exe - C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
msedge.exe
taskhostw.exe - taskhostw.exe SyncFromCloud
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
lsass.exe - C:\Windows\system32\lsass.exe
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS
dwm.exe - "dwm.exe"
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b2d055 /state1:0x41c64e6d
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
taskhostw.exe - taskhostw.exe ExploitGuardPolicy
csrss.exe - %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSyst
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
spoolsv.exe - C:\Windows\System32\spoolsv.exe
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
```

...and 20 more